INFORMATION TECHNOLOGY:
Treasury's Cyber-Based Critical Infrastructure Protection Implementation Efforts Remain Inadequate

OIG-03-093 August 29, 2003

Office of Inspector General

****

The Department of the Treasury

Contents

Appendices

Abbreviations

ATF	Bureau of Alcohol, Tobacco, and Firearms
CIAO	Chief Infrastructure Assurance Officer
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPAMS	Critical Infrastructure Protection Asset Management System
CIPO	Critical Infrastructure Protection Officer
COOP	Continuity of Operations Plan
DO	Departmental Offices
DHS	Department of Homeland Security
DOJ	Department of Justice
ECIE	Economic Council on Integrity and Efficiency
E-ITSPA	Enterprise Information Technology Security Planning and Assurance
FMS	Financial Management Service
FY	Fiscal Year
IT	Information Technology
MEI	Minimum Essential Infrastructure
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General

Contents

PCIE	President’s Council on Integrity and Efficiency
PDD	Presidential Decision Directive
POA&M	Plan of Action and Milestones
TCIPP	Treasury Critical Infrastructure Protection Plan
TIPP	Treasury Infrastructure Protection Panel
Treasury	Department of the Treasury
TT&E	Test, Training, and Exercise
USCS	United States Customs Service
USSS	United States Secret Service

OIG

Audit Report

The Department of the Treasury Office of Inspector General

Drew Ladner
Deputy Assistant Secretary For Information Systems
and Chief Information Officer
Department of the Treasury

The President's Council on Integrity and Efficiency (PCIE)/Economic Council on Integrity and Efficiency (ECIE) Working Group invited the Office of Inspector General (OIG) to participate in a Government-wide review of agency infrastructure assurance programs under Presidential Decision Directive (PDD) 63. As part of the review team, the OIG was requested to conduct an audit of the Department of the Treasury's (Treasury) Cyber-Based Critical Infrastructure Protection (CIP) Implementation.

During our audit, we identified that Treasury did not provide adequate guidance or effective oversight on CIP implementation to the Departmental Offices (DO) or the bureaus. The lack of adequate guidance and effective oversight has impeded Treasury's CIP planning and implementation activities.

The overall objective of this audit was to determine whether Treasury adequately implemented its cyber-based CIP plan under PDD 63. Fieldwork was conducted at DO, the Financial Management Service (FMS), and the United States Customs Service (USCS). In addition, a questionnaire was used to solicit information from the Bureau of Alcohol, Tobacco, and Firearms (ATF) and the United States Secret Service (USSS). A more detailed description of our objective, scope, and methodology is provided in Appendix 1.

On November 25, 2002, President Bush signed the bill to establish the Department of Homeland Security (DHS). With the formation of DHS, certain Treasury CIP cyber assets were transferred to DHS and the Department of Justice (DOJ). Due to the transfer of CIP cyber assets, we recommend that the issues and recommendations identified in this report, which are related to DHS and Justice, be effectively communicated to the appropriate officials at DHS and DOJ.

Results in Brief

We noted that Treasury has made progress in its planning efforts since our last review.[1] Treasury has established the Treasury Infrastructure Protection Panel (TIPP), comprised of representatives from DO and the bureaus. Treasury's Assistant Director for CIP, who also serves as the Critical Infrastructure Protection Officer (CIPO), established a Cyber CIP Working Group, consisting of Treasury, DO and bureau designated CIPOs. In addition, Treasury's CIPO developed the *Treasury Critical Infrastructure Protection Plan (TCIPP), Version 2.0, dated August 30, 2002*, which outlines the Treasury-wide strategy for developing and implementing its CIP program.

We found that Treasury's CIP program continues to need improvement. Treasury did not provide adequate guidance or effective oversight on CIP implementation to DO or the bureaus. The lack of adequate guidance and effective oversight has impeded Treasury's CIP planning and implementation activities. In particular, we noted that:

1. The TCIPP identified a number of documents and tools as key elements to the successful implementation of Treasury's CIP program. However, several of these key elements have not been finalized. Specifically, the CIP Implementation Plan, and the CIP Management Plan remain in draft. Additionally, the CIP Asset Management System (CIPAMS), which is to be used as the Treasury-wide tool for tracking the status of CIP cyber-based assets, has not been developed.

2. The DO and some bureaus have not adequately performed risk management activities. At the USCS, a database is maintained to track the status of systems vulnerabilities identified. We noted that two of the critical cyber-based assets included in the

[1] Review of Treasury's Critical Infrastructure Protection Program, OIG-01-025, dated December 14, 2000.

database had unresolved issues. The USCS is tracking and attempting to resolve these issues. We noted that the USSS was in the process of performing certification and accreditation for all of its systems and major applications, and risk assessments had been conducted for only some of the critical cyber-based systems. Within DO, risk assessments had been completed for only three of its twelve (25 percent) critical cyber-based assets.

3. Treasury has not fully implemented its emergency management plans. We noted that DO and some of the bureaus we reviewed had performed testing of their individual emergency management capabilities. However, the Treasury's Emergency Management Working Group has not validated those test results, and a review of the emergency management program has not been conducted throughout Treasury.

The Treasury CIPO indicated that the Office of the Chief Information Officer (OCIO) did not provide the CIP Program Office with adequate funds and personnel resources to perform oversight and compliance functions. Without adequate resources for its CIP implementation, Treasury cannot ensure that potential risks resulting from security weaknesses will not disrupt the services its critical cyber assets provide for the government, such as revenue collection, law enforcement, and financial management. Additionally, for the Federal Government to attain its goal of achieving full operating capability for protecting the Nation's critical cyber infrastructure by May 2003, every department and agency must comply with the requirements of PDD 63.

Our report includes several recommendations that, in our opinion, will assist Treasury in remedying the deficiencies we identified. We recommend that the Treasury Chief Information Officer (CIO):

- Ensure that funds are appropriated and personnel made available to enable effective implementation of the TCIPP.
- Finalize draft documents that are designated as key elements of the TCIPP and distribute promptly to DO and the bureaus.
- Conduct risk assessments for all critical cyber assets, and develop plans to address any significant vulnerabilities identified.

- Develop a process for DO and the bureaus to report to Treasury on CIP activities, and for Treasury to track the status of vulnerabilities identified in critical cyber assets.
- Conduct a review of cyber disaster recovery capabilities throughout Treasury as soon as possible to ensure that the continuity of operations (COOP) plan is executable.

In its response to our draft report, OCIO management generally concurred with our findings and recommendations. In addition, OCIO management has already commenced efforts to implement our recommendations. Their response is summarized and evaluated in the body of this report and included, in detail, in Appendix 2, Management Comments.

Background

Protection of critical infrastructures remains a high profile issue for the Federal Government. President Bush has declared that securing the nation's critical infrastructures is essential to our economic and national security and is a priority of his administration. Advances in information technology (IT) have caused infrastructures to become increasingly automated and inter-linked. These advancements have created new vulnerabilities related to equipment failures, human errors, weather, and physical and cyber attacks.[2] Non-traditional attacks on our infrastructures and information systems may be capable of significantly harming our economy and military power.

The policy on CIP, PDD 63, issued May 1998, calls for a national effort to assure the security of the nation's critical infrastructures. Critical infrastructures, also known as mission essential infrastructures (MEI[3]), are those physical and cyber systems essential to the minimum operations of the economy and government. Every department and agency is required by PDD 63 to appoint a Chief Infrastructure Assurance Officer (CIAO), who shall be responsible for the planning, development, and implementation of CIP and assurance requirements.

The intent of PDD 63 is that by May 2003, the United States shall have achieved and shall maintain the ability to protect its critical infrastructures from intentional acts that would significantly diminish the abilities of:

- The Federal Government to perform essential national security missions and to ensure the general public health and safety.

[2] Cyber attacks, or cyber terror, may be defined as the unauthorized electronic access, manipulation, or destruction of electronic data or code that is being processed, stored, or transmitted on electronic media, having the effect of actual or potential harm to the nation's critical infrastructure.

[3] The National Critical Infrastructure Assurance Office has defined agency MEI as "the framework of critical organizations, personnel, systems, and facilities that are absolutely required in order to provide the inputs and outputs necessary to support the core processes essential to accomplishing an organization's core mission as they relate to national security, national economic security, or continuity of government services."

- The state and local governments to maintain order and to deliver minimum essential public services.

- The private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services.

Treasury's strategy for protecting its own critical infrastructure is summarized in the TCIPP. The TCIPP divides the responsibility for CIP among Treasury, DO, and the bureaus. Treasury is responsible for the oversight and management of the CIP Program, while DO and the bureaus are responsible for the assurance of critical infrastructures under their purview.

Treasury established the TIPP to facilitate and coordinate the implementation of TCIPP requirements. The TIPP is comprised of representatives from DO and the bureaus, generally the designated CIAO. The TIPP is responsible for developing, formulating, recommending, and establishing the policies, guidelines, plans, and promoting organizational relations for a comprehensive CIP program, as outlined in the TCIPP. Treasury's Enterprise Information Technology Security Planning and Assurance (E-ITSPA) Office, under the Deputy Assistant Secretary for Information Systems and CIO, is charged with developing and overseeing security and emergency management programs to protect Treasury's critical infrastructures.

Finding and Recommendations

Finding

Treasury Did Not Provide Adequate Guidance Or Effective Oversight On CIP Implementation

We found that Treasury did not provide adequate guidance or effective oversight on CIP implementation to DO and the bureaus. Specifically, certain key documents and tools essential to CIP implementation have not been finalized; risk management activities have not been adequately performed; and review of the emergency management program has not been conducted throughout Treasury. The lack of adequate guidance or effective oversight has impeded CIP planning and implementation activities at Treasury. Due to the inability to effectively implement the requirements of

PDD 63, Treasury is unable to ensure that potential risks resulting from security weaknesses will not disrupt the services it provides for the government, such as revenue collection, law enforcement, and financial management. In addition, Treasury is unable to provide the necessary assurance that cyber attacks on its critical infrastructures will not impede its support of national security, national economic security, and national public health and safety.

Key Documents And Tools Essential To CIP Implementation Have Not Been Finalized

The TCIPP indicates that Treasury will rely on certain documents and tools to implement its CIP Program. We noted that some documents identified as key elements in the TCIPP have not been finalized. Specifically, the Treasury CIP Implementation Plan, DO and the bureaus' CIP Management Plans, and the Treasury CIP Management Plan remain in draft. Additionally, the CIPAMS, which will be used as the Treasury-wide tool for tracking the status of CIP cyber-based assets, has not been developed.

Treasury, DO, and the bureaus share the responsibility for developing, implementing, and managing the CIP program. While Treasury's E-ITSPA is responsible for oversight and management of the program, DO and each bureau are required to develop their own CIP Management Plan following the guidance provided in the TCIPP and the Treasury CIP Implementation Plan. At the time of our review, the Treasury CIP Implementation Plan remained in draft.

Per the TCIPP, Treasury is to rely on the following key elements to implement the Treasury CIP Program:

- <u>Treasury CIP Implementation Plan</u> - The Treasury CIP Implementation Plan, version 1.3 (dated April 24, 2000), remains in draft. The CIP Implementation Plan provides additional guidance for achieving the Treasury CIP Policy and to help DO and the bureaus meet the CIP requirements.

- <u>DO and Bureaus' CIP Management Plans</u> - The CIP Management Plans for DO and the bureaus will address their respective CIP-related goals, which should include governance, risk management, critical asset management, threat assessment, risk assessment, business continuity planning and management, incident reporting and handling, and training and awareness. However, neither DO nor the bureaus we reviewed had received the appropriate guidance from Treasury for developing a CIP Management Plan. Therefore, neither DO nor the bureaus reviewed has completed a CIP Management Plan.

- Treasury CIP Management Plan - The Treasury CIP Management Plan is to focus on such issues as common threats, vulnerabilities, and interdependencies identified in DO and the bureaus' CIP Management Plans. The DO and the bureaus' CIP Management Plans form the basis of the Treasury CIP Management Plan; and since those have not been completed, the Treasury CIP Management Plan remains in draft.

- CIPAMS - The centralized database, CIPAMS, which is to be used for the collection of consistent and comparable data regarding CIP assets, has not been developed. The CIPAMS will include critical asset data such as threats and vulnerabilities, remediation strategy, estimated cost, and remediation schedule. This system will facilitate the availability of current and accurate information about the status of DO and bureaus' critical assets.

Risk Management Activities Have Not Been Adequately Performed

Treasury requires DO and each of the bureaus to develop a risk management plan to define and perform activities for their unique operations. The risk management plan, as described in the TCIPP, encompasses two key components—risk assessment and risk mitigation. The risk assessment is used to determine the extent of the potential threats and risks associated with an IT system throughout its life cycle. Risk mitigation is the process of prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.

The DO and some of the bureaus have not adequately performed risk management activities necessary to protect their critical cyber assets. We noted that the USCS maintains a database to track the status of vulnerabilities identified for its cyber-based assets. The database contains background information on the vulnerabilities, as well as mitigation plans and the status of the plans. We found that the database included two critical cyber-based assets for which certain vulnerabilities were identified, but mitigation plans had not been developed. The USSS was in the process of performing certification and accreditation of all of its systems and major applications; and at the time of our review, risk assessments had been conducted for only some systems. Within DO, risk mitigation plans had been completed for only three of its twelve (25 percent) critical cyber-based assets. Without conducting risk assessments for critical assets and completing risk mitigation plans to address identified vulnerabilities, Treasury will not be aware of the potential risks and weaknesses related to its critical assets.

We noted that DO and the bureaus are required to report critical asset data to Treasury's CIPO. However, the CIPO indicated that the CIP Program Office did not have sufficient personnel or tools to ensure that DO and the bureaus comply with those requirements. According to the CIPO, the CIP Program Office has been focusing on program management activities, such as developing guidance and policy documents. Furthermore, the CIPAMS, which will collect data on vulnerabilities associated with CIP assets, has not been developed.

Emergency Management Plans Have Not Been Fully Implemented

Despite on-going activities to improve Treasury's IT security program, the OCIO has not fully implemented its emergency management program. While DO and some of the bureaus have tested various aspects of their respective emergency plans, a comprehensive test of the cyber CIP disaster recovery capabilities throughout Treasury has not been conducted. Without conducting a comprehensive test of the emergency management plan, Treasury cannot ensure that DO and the bureaus have viable COOP capabilities. Treasury lacks adequate personnel resources to coordinate and oversee the emergency management activities throughout Treasury.

Treasury's draft Emergency Management Test, Training and Exercise (TT&E) Program policy states that the goal of the program is to "ensure, as a baseline of preparedness, that the Department has in place a viable COG [continuity of Government] and COOP capability that ensures the performance of its *essential functions* during any emergency or situation…" One of the goals of the TT&E Program is to conduct "testing and exercising of the COOP plans and procedures to test and exercise interoperability between and among Treasury HQ [headquarters] and bureau COOP teams, as well as to test and exercise the ability of these COOP teams to perform their essential functions and operate from their AOFs [alternate operating facilities]." The TT&E Program policy emphasizes that the goal of having a successful TT&E Program in place is "possible only if training and exercising are conducted on a regular schedule…." Per the National Institute of Standards and Technology's *Generally Accepted Principles and Practices for Securing Information Technology Systems,* an organization should test and revise the emergency plan.

The lack of adequate guidance and effective oversight is attributed largely in part to the fact that Treasury has not adequately funded its current PDD 63 effort. The OIG has previously reported on inadequate funding and resources being devoted to Treasury's CIP Program[4]. Treasury committed funds in Fiscal Year (FY) 2002 for CIP planning activities and to implement the strategy detailed in the TCIPP. However, not all of the funds committed were actually provided to the CIP Program Office. Treasury's report on IT spending, (Exhibit 53), appropriated $5.7 million for Treasury-wide CIP activities in FY 2002. However, only $1.5 million was received for the CIP Program in FY 2002. Consequently, some CIP activities planned during the year were not undertaken. For example, although $1.7 million was slated for oversight capability, none of the funds that were received went toward oversight. Additionally, only $300,000 of the $910,000 earmarked for vulnerability tools/test lab was received.

In addition to inadequate funding for CIP Implementation at Treasury, there are limited personnel resources devoted to CIP Program activities. At the time of our review, the cyber CIP Program Office at Treasury consisted of only two personnel, including the CIPO. The CIP Program Office has identified that two additional personnel were needed to accomplish the mission of the program, but requests made by the CIP Program Office to

[4] Review of Treasury's Critical Infrastructure Protection Program, *OIG-01-025, dated December 14, 2000.*

Treasury’s E-ITSPA Director for the additional personnel have been declined.

Recommendations

Treasury’s CIO should:

1. Ensure that funds are appropriated and personnel made available to enable effective implementation of the TCIPP.

   Management Response:

   OCIO management concurred with our recommendation. Although the staff supporting the Treasury-wide CIP program was divested to DHS, the OICO remains committed to ensuring that the necessary personnel and funds will be allocated for the CIP program. OCIO management recently justified continued appropriated funding for FY 2004 funding for the CIP program.

2. Finalize draft documents that are key elements of the TCIPP and distribute them to DO and the bureaus, ensuring that DO and the bureaus have the necessary guidance to comply with PDD 63 requirements.

   Management Response:

   OCIO management concurred with our recommendation. Documents identified as key elements of the TCIPP were either finalized and distributed to the bureaus, or are currently in the process. Also, the Treasury CIP policy was incorporated into Treasury’s comprehensive IT Security Policy manual and distributed to the bureaus in June 2003. The draft Treasury CIP Implementation Plan was updated as of February 24, 2003; however, OCIO management is in the process of determining the applicability of issuing the document given the new direction of the National CIAO. Finally, OCIO management plans to develop the Treasury CIP Management Plan after they have conducted Project Matrix Step 2.

3. Conduct risk assessments for all critical cyber assets, and develop plans to address the significant vulnerabilities identified in order to mitigate security exposures.

Management Response:

OCIO management generally concurred with our recommendation. All bureaus having critical cyber assets are required to develop plans to address significant vulnerabilities. These vulnerabilities should be addressed through Treasury's requirement for all systems being certified and accredited. Any vulnerability identified during the certification and accreditation process is tracked with the Department's Plan of Action and Milestones (POA&M) reporting procedures. OCIO management plans to identify CIP cyber assets separately in its POA&M reporting.

4. Develop a process for DO and bureaus to report to Treasury on CIP activities and for Treasury to track the status of vulnerabilities identified in critical cyber assets.

   Management Response:

   OCIO management generally concurred with our recommendation. OCIO management plans to track the status of vulnerabilities identified for CIP cyber assets through the POA&M reporting process. Confirmation that appropriate action has occurred will be assured through the Security Oversight and Compliance Program.

5. Conduct a review of cyber disaster recovery capabilities throughout Treasury as soon as possible to ensure the COOP plan is executable.

   Management Response:

   A security program review of each bureau's IT security program is nearing completion to meet an instituted FY 2003 CIO oversight goal. Reviewing each bureau's cyber disaster recovery capability is an integral part of the security program review. The Emergency Preparedness Office, under the direction of the Senior Advisor to the Assistant Secretary for Management / Chief Financial Officer, has met with the bureaus and received individual bureau COOP plans for review. The

> Emergency Preparedness Office has the vital function of monitoring the execution of the bureaus' COOP plans.

OIG Comment:

The OIG agrees that the formal steps Treasury management has taken, and plans to take, satisfy the intent of the recommendations.

* * * * * *

I would like to extend our appreciation to the Treasury for the cooperation and courtesies extended to my staff during the review. If you have any questions, please contact me at (202) 927-5774, or Joseph Maranto, Audit Manager, at (202) 927-0191. Major contributors to this report are listed in Appendix 3.

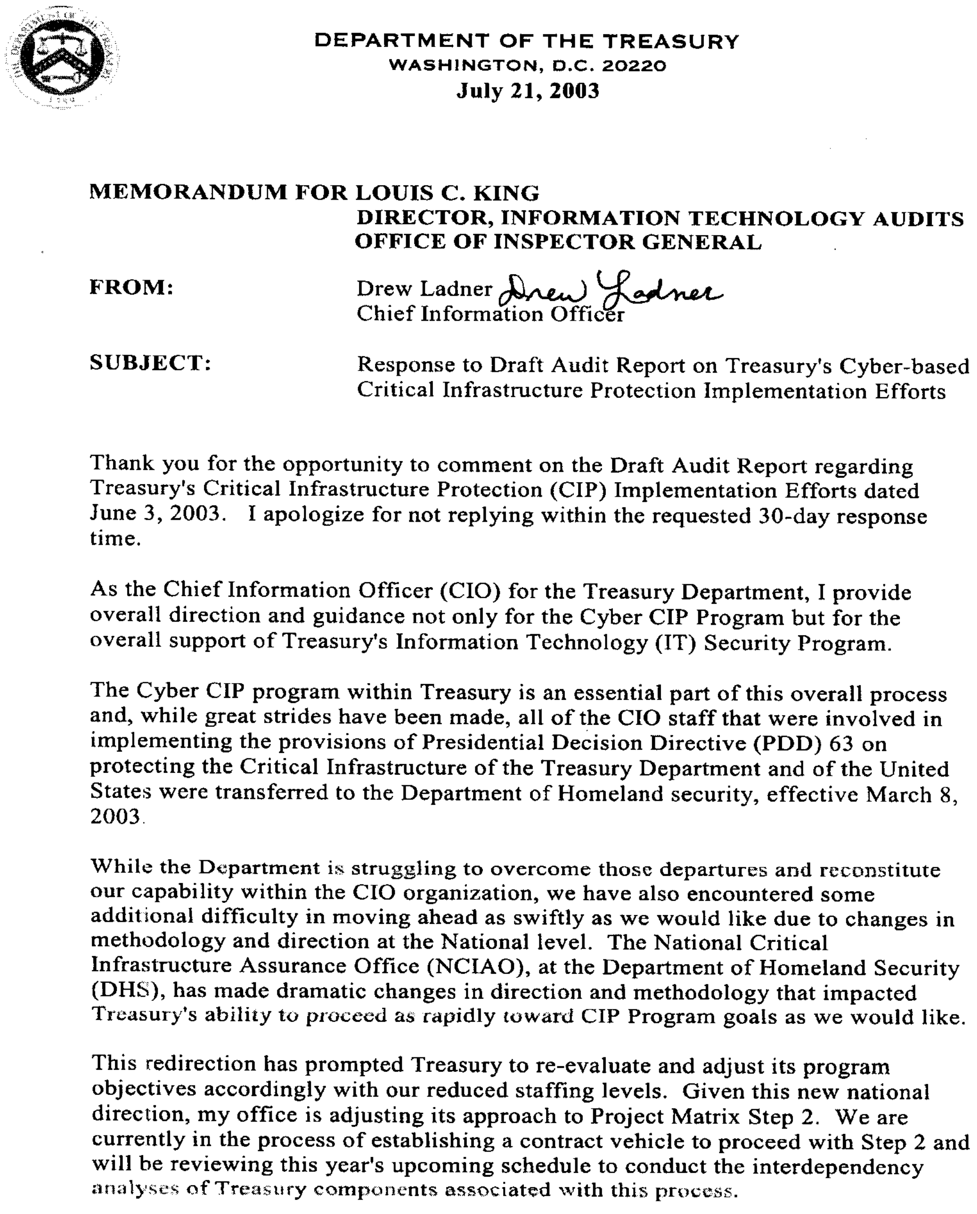
/s/
Louis C. King
Director, Information Technology Audits

The overall objective of this review was to determine whether Treasury has adequately implemented its cyber-based CIP plan under PDD 63. Specifically, we determined the adequacy of Treasury's implementation activities in the following areas: (1) risk mitigation; (2) emergency management; (3) interagency coordination; (4) resource and organization requirements; and (5) recruitment, education, and awareness.

Our work was part of a larger effort by the PCIE/ECIE to monitor CIP programs across the Federal Government. To allow our results to be consolidated with those of other Federal Agency Offices of Inspector General and reported on a Government-wide basis, we used the PCIE/ECIE Review Guide, Phase II, dated April 2002.

We identified 18 critical cyber assets as our audit universe, based upon our review of Treasury's Project Matrix Step 1 Report, dated October 2000. The components with critical cyber assets were selected for review. Fieldwork was performed at the Treasury OCIO, DO, FMS, and the USCS from October through December 2002. Additionally, an audit questionnaire was used to solicit information on implementation activities at ATF and the USSS.

We conducted our audit in accordance with generally accepted government auditing standards.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220
July 21, 2003

MEMORANDUM FOR LOUIS C. KING
DIRECTOR, INFORMATION TECHNOLOGY AUDITS
OFFICE OF INSPECTOR GENERAL

FROM: Drew Ladner Drew Ladner
Chief Information Officer

SUBJECT: Response to Draft Audit Report on Treasury's Cyber-based Critical Infrastructure Protection Implementation Efforts

Thank you for the opportunity to comment on the Draft Audit Report regarding Treasury's Critical Infrastructure Protection (CIP) Implementation Efforts dated June 3, 2003. I apologize for not replying within the requested 30-day response time.

As the Chief Information Officer (CIO) for the Treasury Department, I provide overall direction and guidance not only for the Cyber CIP Program but for the overall support of Treasury's Information Technology (IT) Security Program.

The Cyber CIP program within Treasury is an essential part of this overall process and, while great strides have been made, all of the CIO staff that were involved in implementing the provisions of Presidential Decision Directive (PDD) 63 on protecting the Critical Infrastructure of the Treasury Department and of the United States were transferred to the Department of Homeland security, effective March 8, 2003.

While the Department is struggling to overcome those departures and reconstitute our capability within the CIO organization, we have also encountered some additional difficulty in moving ahead as swiftly as we would like due to changes in methodology and direction at the National level. The National Critical Infrastructure Assurance Office (NCIAO), at the Department of Homeland Security (DHS), has made dramatic changes in direction and methodology that impacted Treasury's ability to proceed as rapidly toward CIP Program goals as we would like.

This redirection has prompted Treasury to re-evaluate and adjust its program objectives accordingly with our reduced staffing levels. Given this new national direction, my office is adjusting its approach to Project Matrix Step 2. We are currently in the process of establishing a contract vehicle to proceed with Step 2 and will be reviewing this year's upcoming schedule to conduct the interdependency analyses of Treasury components associated with this process.

Report findings and recommendations:

In your report, you specifically note that (1) certain key documents and tools essential to CIP implementation were not finalized; (2) risk management activities were not adequately performed by the Departmental Offices and some bureaus; and (3) emergency management plans were not fully implemented.

I would like to address each of these areas separately and then discuss the corresponding recommendations.

1. **Certain key documents and tools essential to CIP implementation were not finalized.**

   The draft report specifically addresses that three elements have not been finalized. These elements are the Treasury CIP Policy, the CIP Implementation Plan, and the CIP Management Plan. Additionally, the report discusses the development of a CIP Asset Management System which would be used as a Treasury-wide tool for tracking the status of CIP cyber-based assets.

   a. Treasury CIP Policy - The Treasury CIP Policy has been incorporated into Treasury's comprehensive IT Security Policy manual (TD P 85-01). The preliminary version of this policy was electronically distributed to the bureaus in June 2003. An HTML version of the policies and associated handbooks will be posted on Treasury's Enterprise IT Security Planning and Assurance website. We will be pleased to provide a soft copy to your office for your records.

   b. CIP Implementation Plan - The draft audit report references a CIP Implementation Plan, version 1.3 (dated April 24, 2000); however, there is a later draft dated February 24, 2003, that is available for your review. It should be noted, however, my office is currently in the process of determining the applicability of issuing this document given the new direction by DHS-NCIAO. It may be in the best interest of the Treasury Department and the general public not to issue the document.

   c. Treasury CIP Management Plan - As appropriately identified in your audit report, the Treasury CIP Management Plan is formulated based upon common threats, vulnerabilities, and interdependencies identified throughout the Treasury components. Further, as stated in the draft audit report, these actions then form the basis of the Treasury CIP Management Plan. Accordingly, the Management Plan will be developed after we have conducted Project Matrix Step 2 from which common threats and vulnerabilities will be identified through the Treasury interdependency analyses process.

d. CIP Asset Management System - Finally, under item 1 of Results in Brief, the report discusses the development of a CIP Asset Management System which would be used as a Treasury-wide tool for tracking the status of CIP cyber-based assets. The report discusses this element as a distinguishable system that is required to track the status of CIP cyber-based assets. With the on-going development and strengthening of the Department's IT Security Program, we have incorporated the tracking of CIP cyber-based assets into a tracking and monitoring system developed for actions associated with requirements of the Federal Information Security Management Act (FISMA). We are currently in the process of identifying the Treasury Critical Systems within this tracking system and cross matching vulnerabilities and weaknesses associated with the critical systems against the Plans of Actions and Milestones (POA&MS) submitted by Treasury bureaus. This will ensure we not only track the critical systems but that we also ensure they are certified and accredited to operate according to Treasury policy and that any weaknesses are re-mediated.

2. **The DO and some bureaus have not adequately performed risk management activities.**

The draft audit report notes that within the Departmental Offices only three of its twelve critical cyber-based assets have had risk assessments completed. We are in the process of reviewing the status of systems within DO identified as critical cyber-based assets and will ensure that risk assessments are completed as a component of the Certification and Accreditation effort required for FISMA compliance. As soon as this effort is completed, we will be pleased to provide the findings to your office.

The draft report also states a database at the United States Customs Service is maintained to track the status of system vulnerabilities identified; however, two of the critical cyber-based assets included in the database had unresolved issues. Additionally, it was noted that certification and accreditation and risk assessments at the United States Secret Service were conducted for only some of critical cyber-based systems. As both of these bureaus have formally been transferred to the Department of Homeland Security, my office no longer has oversight responsibility for these areas.

3. **Treasury has not fully implemented its emergency management plans.**

We believe this finding should be directed to the appropriate Treasury organizational component that has overall responsibility for emergency preparedness within the Department. My office does not have direct responsibility for emergency preparedness; however, we are currently addressing disaster recovery issues for Treasury cyber assets through the FISMA POAM process. This year, my office will specifically address whether bureaus have disaster recovery plans in place through our compliance review efforts.

The next section addresses the final recommendations of the draft audit report found on page 14.

1. **Ensure that funds are appropriated and personnel made available to enable effective implementation of the Treasury CIP Plan (TCIPP).**

   The formulation of the Department of Homeland Security resulted in the loss of the entire federal staff supporting implementation of the Treasury-wide Critical Infrastructure Protection program. However, you have my commitment that my office will undertake efforts to reconstitute the appropriate personnel and funds to ensure that the CIP program is not identified as having a material weakness. My office recently justified continued appropriated funding for FY 2004 to provide the foundation of a viable program.

2. **Finalize draft documents that are key elements of the TCIPP and distribute them to DO and the bureaus, ensuring that DO and the bureaus have the necessary guidance to comply with PDD 63 requirements.**

   As indicated earlier in this response, some of the documents identified in the audit report as currently in draft status have been issued. My office would be pleased to provide you with final issuances of these documents for your records. In addition to the draft documents mentioned in the draft report, it should also be noted the Department has issued two other final documents related to the CIP program. These documents are the Treasury Critical Infrastructure Protection Plan (TCIPP), Version 2, dated August 30, 2002; and the Treasury Critical Infrastructure Protection: Interdependency Analysis Methodology, Version 1.1, dated September 24, 2002. My office would be pleased to provide copies of these reports as well for validation and verification.

3. **Conduct risk assessments for all critical cyber assets, and develop plans to address the significant vulnerabilities identified in order to mitigate security exposures.**

   Currently all bureaus that have critical cyber assets are required to develop plans to address significant vulnerabilities. This is principally addressed through Treasury's requirement to have all Treasury systems certified and accredited. Any vulnerability identified during the certification process is tracked by the Department through the POAM tracking process. The Treasury Critical Systems are in the process of being identified separately in this tracking system to ensure measures are taken to mitigate security exposure.

4. **Develop a process for DO and the bureaus to report to Treasury on CIP activities and for Treasury to track the status of vulnerabilities identified in critical cyber assets.**

   In the future, Treasury will incorporate the reporting of CIP activities into the joint Treasury OIG and CIO data call for FISMA and will continue to track these activities through the POAM reporting process. As is currently planned, the confirmation that appropriate action has occurred will be assured through the Security Oversight and Compliance Program.

5. **Conduct a review of cyber disaster recovery capabilities throughout Treasury as soon as possible to ensure the COOP plan is executable.**

   A Security Program Review of each bureau's IT security program is nearing completion to meet an instituted FY 2003 CIO oversight goal. An integral part of the reviews addresses the bureau's cyber disaster recovery capabilities. The results serve as a baseline for each bureau's IT contingency planning capability and consist of the development, implementation and scope of IT security contingency plans. Reviews will be performed to ensure the plans incorporate a business impact analysis, standard operating procedures, emergency management, disaster recovery, continuity of operations and other related contingency tactics. The Emergency Preparedness Office under the direction of the Senior Advisor to the Assistant Secretary for Management/CFO has met with the bureaus and received individual bureau COOP plans for review. The Emergency Preparedness Office has the vital function of monitoring the execution of the bureaus' COOP plans.

I would again like to thank you for the opportunity to comment on the draft audit report. Should you have any questions, please do not hesitate to contact me at (202) 622-1200 or Michelle Moldenhauer, Director, Security Compliance at (202) 622-1110.

Office of Information Technology Audits

Edward G. Coleman, former Director, Office of IT Audits
Joseph Maranto, IT Audit Manager
Patrick Nadon, IT Audit Manager
Sandra Turgott, Team Lead
Richard Kernozek, IT Auditor
Anthony Nicholson, IT Auditor
Angela Payton, Computer Specialist
Tram Do, Referencer
Kenneth Harness, Referencer

The Department of the Treasury

Office of the Deputy Assistant Secretary for Information Systems/Chief Information Officer
Enterprise IT Security Planning and Assurance
Office of Accounting and Internal Control

Office of Management and Budget

Office of Inspector General Budget Examiner

Other

President's Council on Integrity and Efficiency